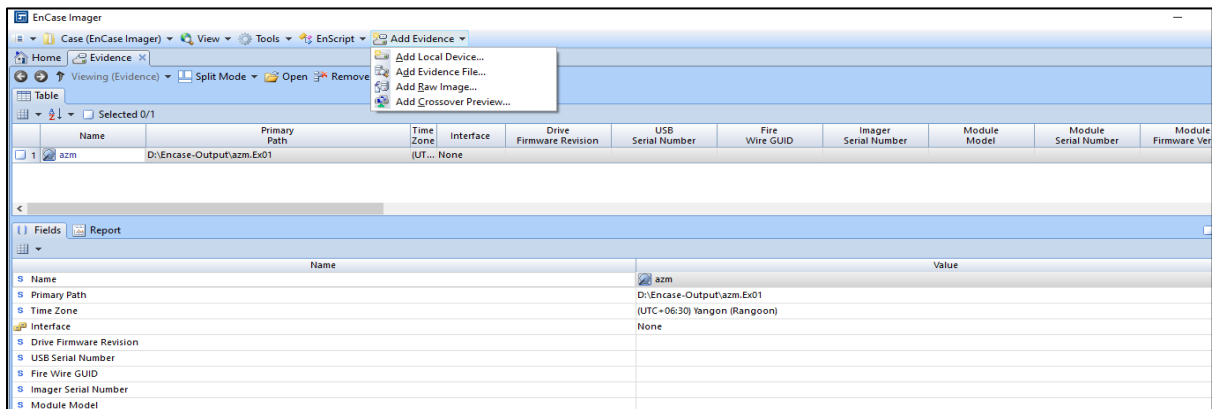
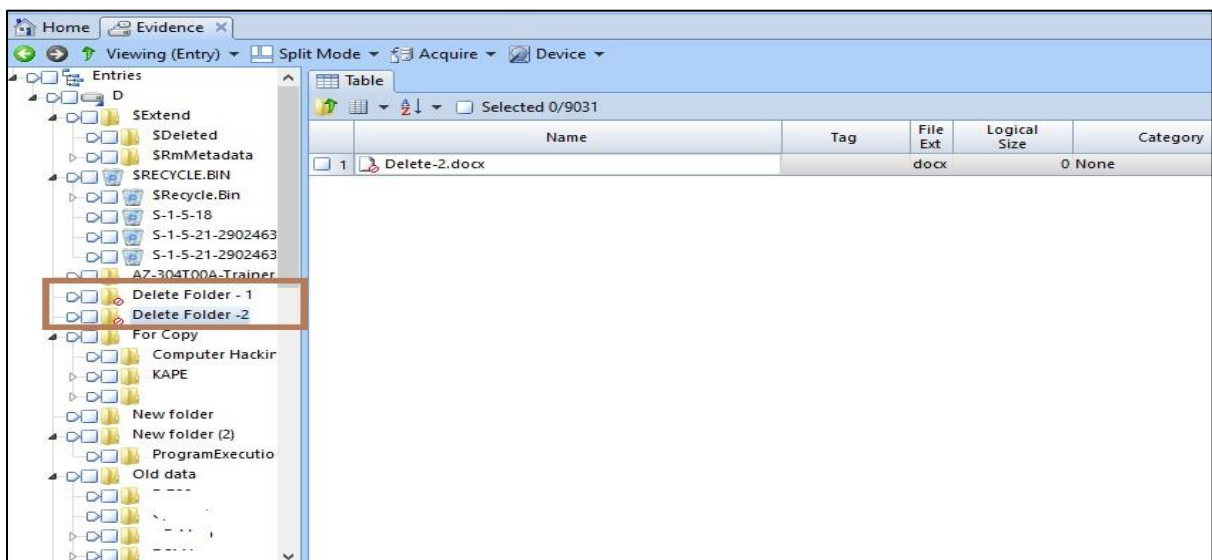


အခု PDF လေးကတော့ Digital Forensics Acquisition Process With FTK Imager ရဲ့အဆက်ဖြစ်ပါတယ်။ ဘာလို့ Example ပြတာကို Open Source ဖြစ်တဲ့ FTK Imager နဲ့ပြသလဲဆိုတာကို ထပ်မံရှင်း လင်းတာ ဖြစ်ပါတယ်။ FTK Imager က Open Source ဖြစ်ပေမဲ့ Commercial Version မှာဆိုရင် နာမည်ကြီး ပဲဖြစ်ပါတယ်။ Commercial Version က နည်းနည်းလေးပဲ FTK Imager နဲ့ကွဲပြားပါတယ်။ Process နဲ့လုပ်ပုံလုပ်နည်းက တော်တော်များများတူညီပါတယ်။ လုပ်ငန်းခွင်မှလူများ နဲ့ ကျောင်းသား ကျောင်းသူများ အတွက် လေ့လာ အသုံးပြုတဲ့ အခါမှာ စရိတ်သက်သာအောင် Open Source ဖြစ်တဲ့ FTK နဲ့ ဥပမာပေးပြီး ရေးသားခဲ့တာဖြစ်ပါတယ်။

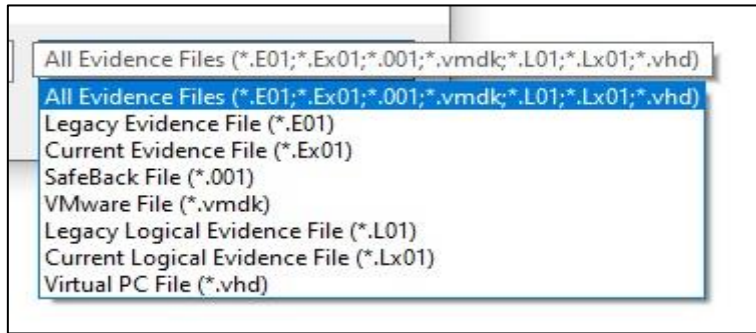
Encase Imager ကတော့ Computer Forensics မှာ နာမည်ကြီးတဲ့ Encase (Open Text) က Imager ဖြစ်ပါတယ်။ Open Source မဟုတ်ပဲ Commercial Version ဖြစ်ပါတယ်။



Encase Imager



Evidence Add ပြီးတာနဲ့ Delete လုပ်ထားတဲ့ File Folder တွေကို Encase မှာလဲကြည့်နိုင်ပါတယ်။



အခြားသော Forensics Image, Disk Image တွေကိုလဲ Support ပေးပါတယ်။ သူ့ထဲမှာ Add ပြီးကြည့်နိုင်ပါတယ်။

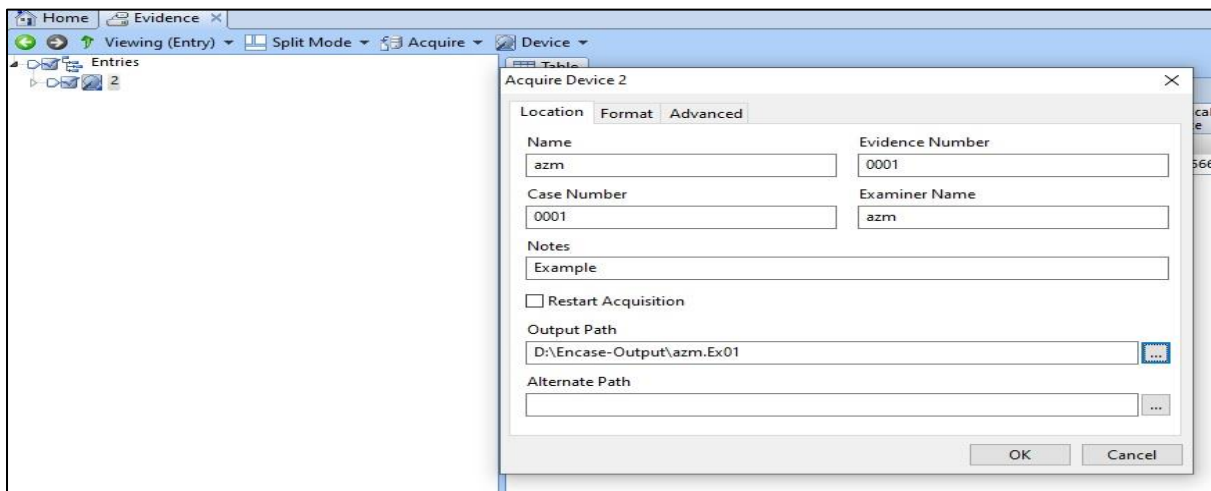


Image လုပ်တဲ့နေရာမှာ လုပ်ဆောင်ရတဲ့ Process က FTK Imager ပုံစံအတိုင်းဖြစ်ပါတယ်။

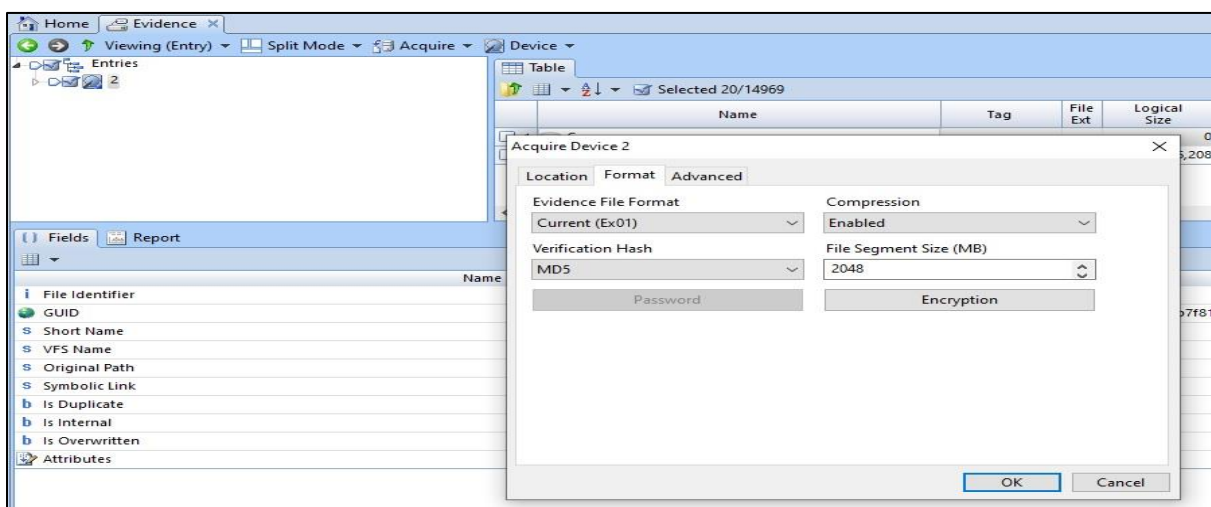
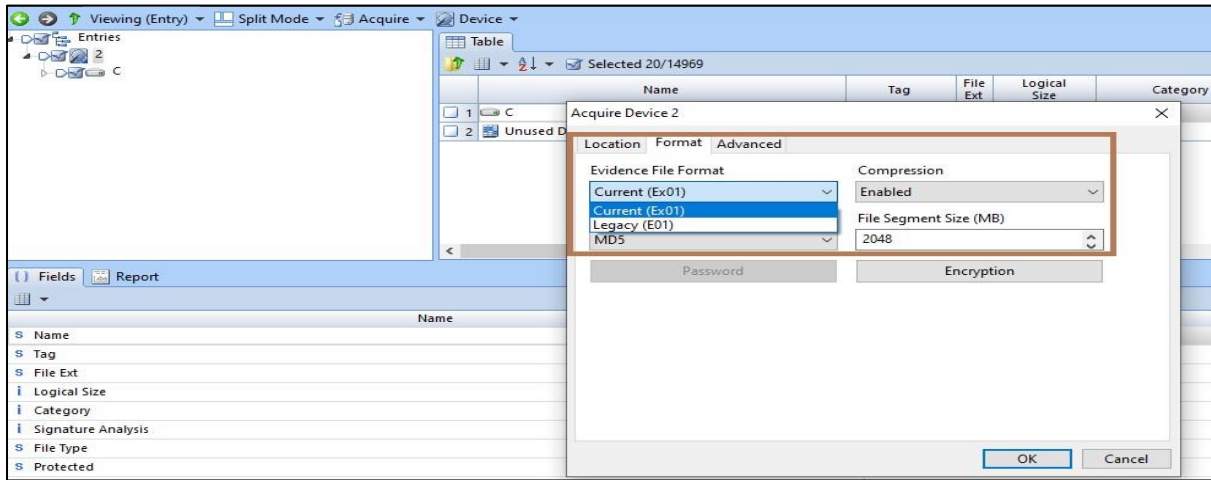


Image လုပ်တဲ့နေရာမှာ လုပ်ဆောင်ရတဲ့ Process က FTK Imager ပုံစံအတိုင်းဖြစ်ပါတယ်။



Disk Image ကို Segment လေးတွေပိုင်းခြားနိုင်တာကလဲ FTK ပုံစံအတိုင်းဖြစ်ပါတယ်။

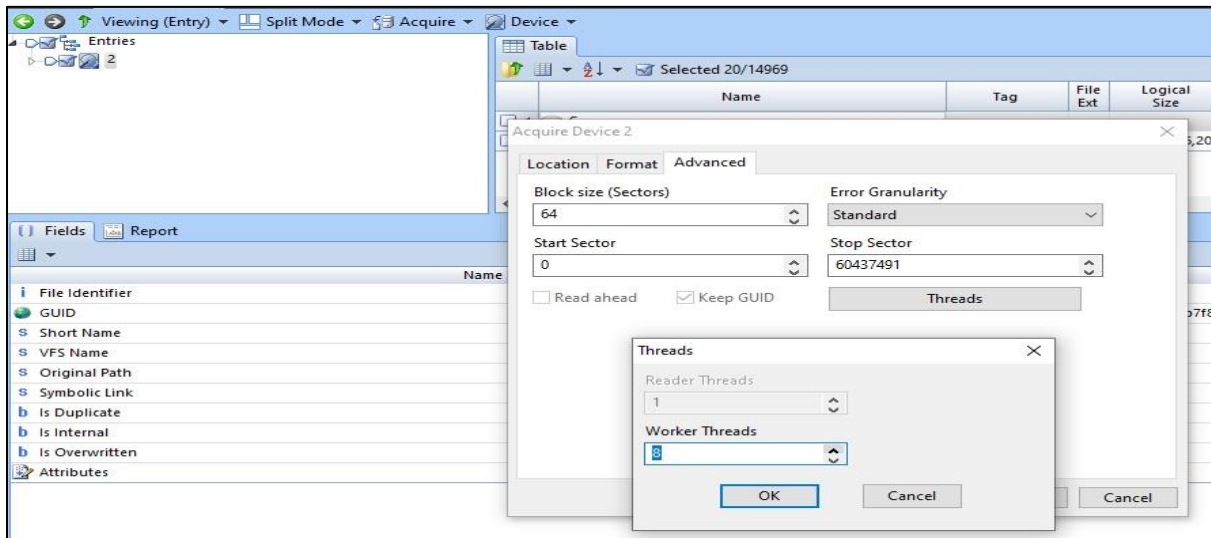
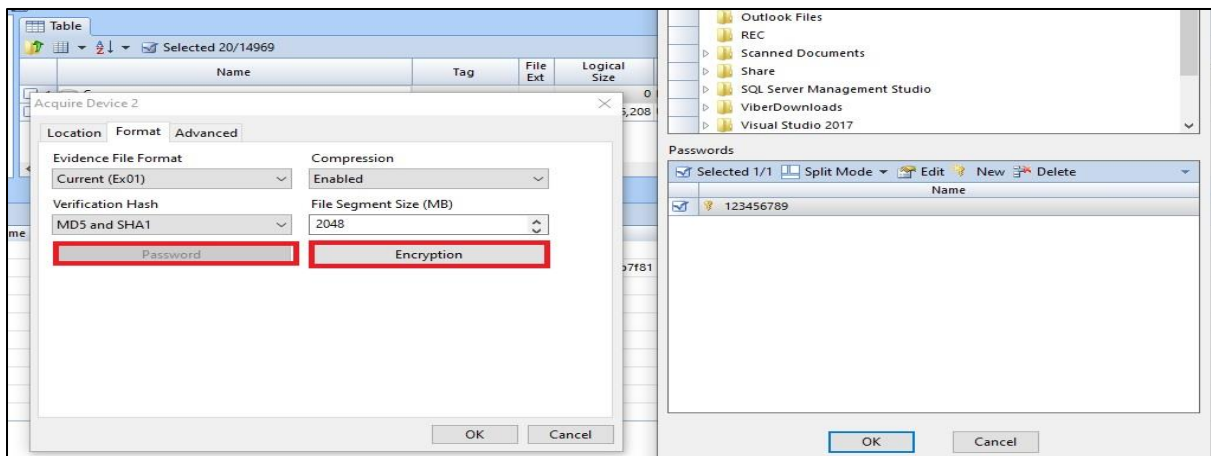


Image လုပ်တဲ့အချိန်မှာ CPU Threads ခွဲနိုင်တာတော့ ကွာခြားပါတယ်။



FTK Imager မှာလိုပဲ Disk Image ဒါမှမဟုတ် Image လုပ်တဲ့ File , Folder ကို Password Encryption ပေးနိုင်ပါတယ်။

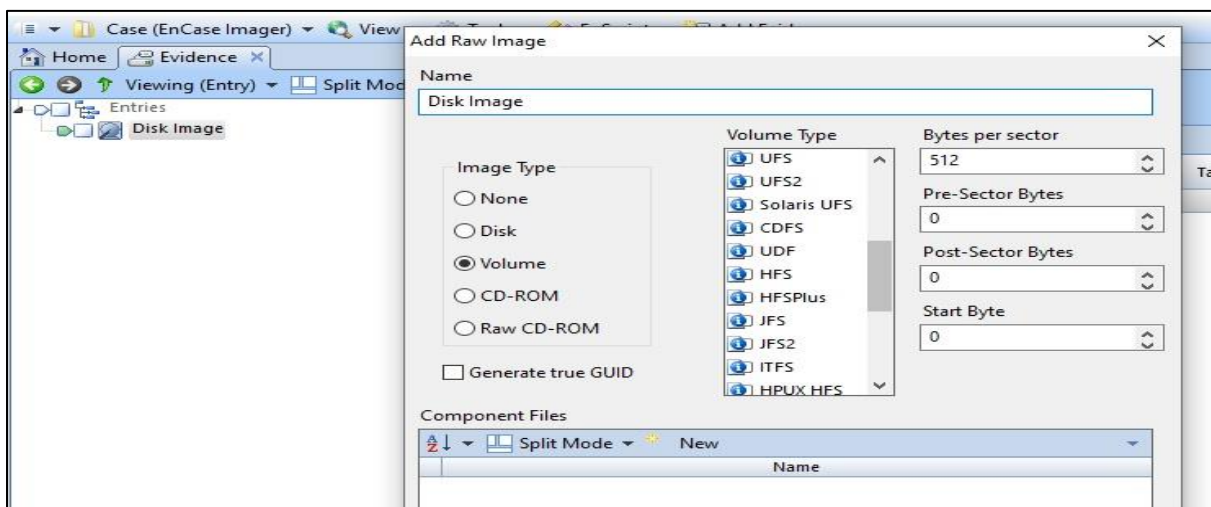
1	azm	D:\Encase-Output\azm.Ex01	(UT... None			
2	000	D:\Encase-Output\azm.Ex01	(UT... None			
3	USB-1	D:\Encase-Output\azm.Ex01	(UT... None			

Fields	Report
Name	
S Label	Kingston
S Serial Number	E0D55E6CE772F491A91868D9
S Model	DataTraveler 3.0
b Read File System	.
b Parse Link Files	.
Drive Type	Detachable
Open Mode	Evidence File
Source Type	Evidence File2
Actual Date	03/06/22 06:51:27 PM
Target Date	03/06/22 06:51:28 PM
S Case Number	0001
S Examiner Name	azm
S Evidence Number	0001
S Notes	Example
S File Integrity	Completely Verified, 0 Errors
Acquisition MD5	3a5b3a55769ba640a4d02877198eb366
Verification MD5	3a5b3a55769ba640a4d02877198eb366

Image ပြီးတဲ့အချိန် လုပ်ထားတဲ့ Image File ကိုထည့်ကြည့်ရင် အခုလိုပုံစံမျိုးမြင်ရမှာဖြစ်ပါတယ်။
FTK နဲ့ပုံစံတူပါတယ်။

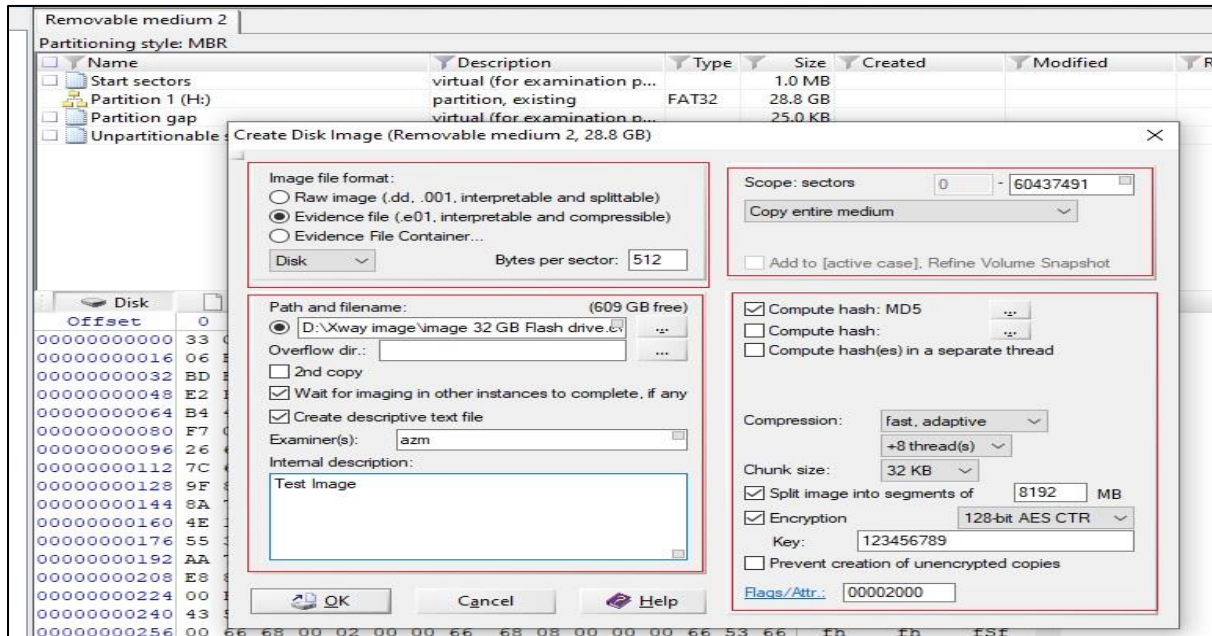
Name	Date modified	Type	Size
azm.Ex01	3/6/2022 6:52 PM	EX01 File	2,097,886 KB
azm.Ex02	3/6/2022 6:52 PM	EX02 File	2,097,864 KB
azm.Ex03	3/6/2022 6:53 PM	EX03 File	2,097,857 KB
azm.Ex04	3/6/2022 6:54 PM	EX04 File	2,097,861 KB
azm.Ex05	3/6/2022 6:54 PM	EX05 File	2,097,889 KB
azm.Ex06	3/6/2022 6:55 PM	EX06 File	2,097,874 KB
azm.Ex07	3/6/2022 6:56 PM	EX07 File	2,097,884 KB
azm.Ex08	3/6/2022 6:56 PM	EX08 File	2,097,856 KB
azm.Ex09	3/6/2022 6:57 PM	EX09 File	2,097,866 KB
azm.Ex10	3/6/2022 6:58 PM	EX10 File	2,097,873 KB
azm.Ex11	3/6/2022 6:58 PM	EX11 File	2,097,879 KB
azm.Ex12	3/6/2022 6:59 PM	EX12 File	2,097,874 KB
azm.Ex13	3/6/2022 7:00 PM	EX13 File	2,097,884 KB
azm.Ex14	3/6/2022 7:00 PM	EX14 File	2,097,878 KB
azm.Ex15	3/6/2022 7:01 PM	EX15 File	435,097 KB
Example-Key .PublicKey	3/6/2022 6:59 PM	PUBLICKEY File	2 KB

Encase ကနေ Image လုပ်ပြီးတဲ့အချိန် ထွက်လာတဲ့ Output Image ပုံစံဖြစ်ပါတယ်။

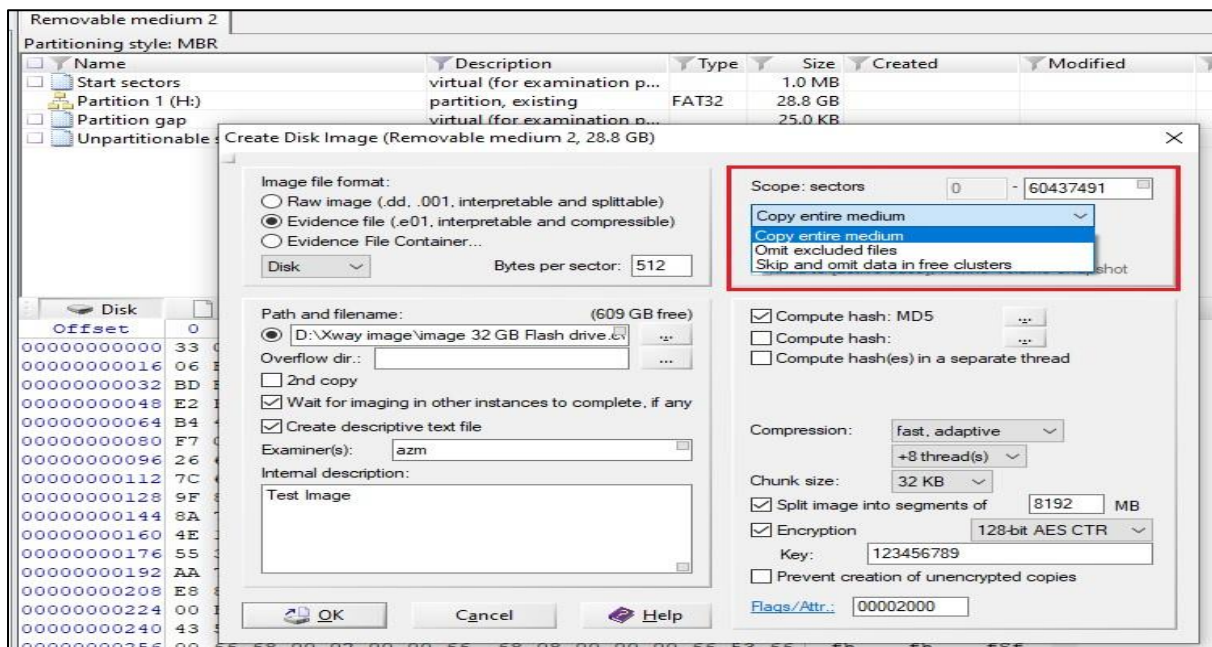


အခြားသော Disk Image Type, File Type တွေကို Encase မှာထည့်ကြည့်နိုင်ပါတယ်။ FTK မှာပါတဲ့ပုံစံအတိုင်းပဲ ဖြစ်ပါတယ်။

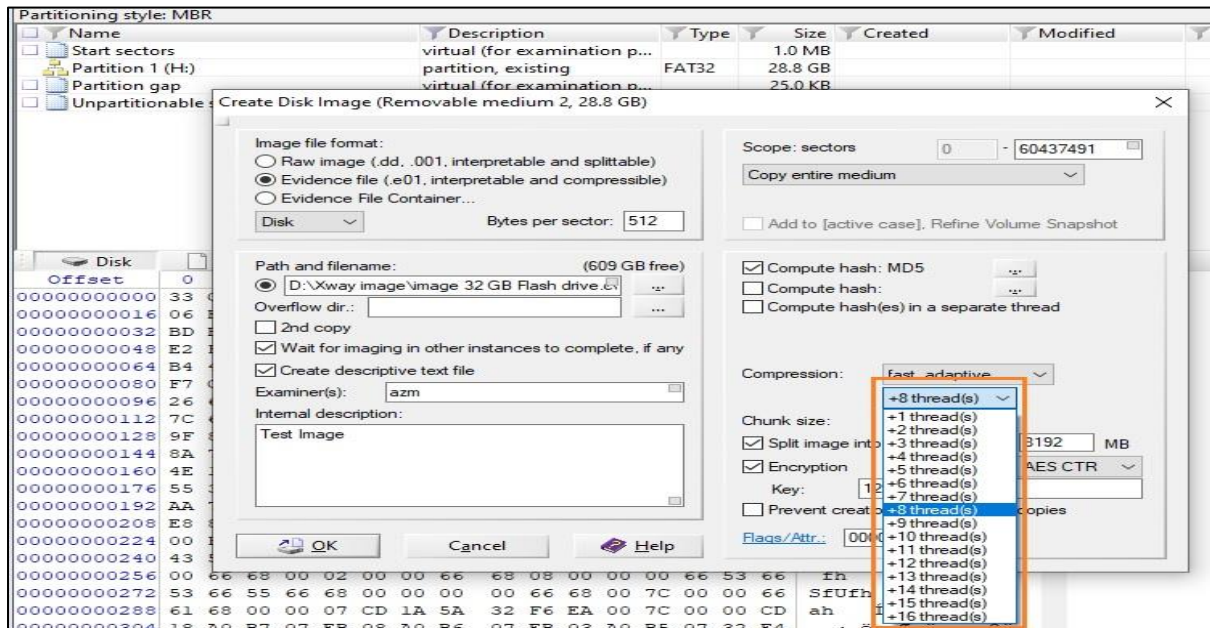
နောက်တစ်ခုကတော့ Commercial Version တစ်ခုဖြစ်တဲ့ X-Way Forensics မှာပါတဲ့ X-Way Imager ပဲဖြစ်ပါတယ်။ ပုံစံကိုကြည့်လိုက်ရင် FTK Imager မှာပါတဲ့ ပုံစံအတိုင်းဖြစ်ပါတယ်။ Raw (dd) ရမယ်။ e01 File Type ကို Image လုပ်လို့ရမယ်။ Hash Compute, Hash Verify, Encryption ပါမယ်။ Image File ကို segment အပိုင်းလေးတွေခွဲတာပါပါမယ်။



X-Way Imager



FTK နဲ့မတူတာက Disk Free Space တွေကို ကိုယ့်လိုအပ်ချက်အရ Image မယူပဲ ကျော်နိုင်ပါတယ်။ အချိန်ကုန်သက်သာစေဖို့ဖြစ်ပါတယ်။



FTK နဲ့မတူပဲ Encase နဲ့တူတာက Workstaion အပေါ်မူတည်ပြီး Imaging လုပ်တဲ့ Process ကို Thread ခွဲနိုင်ပါတယ်။

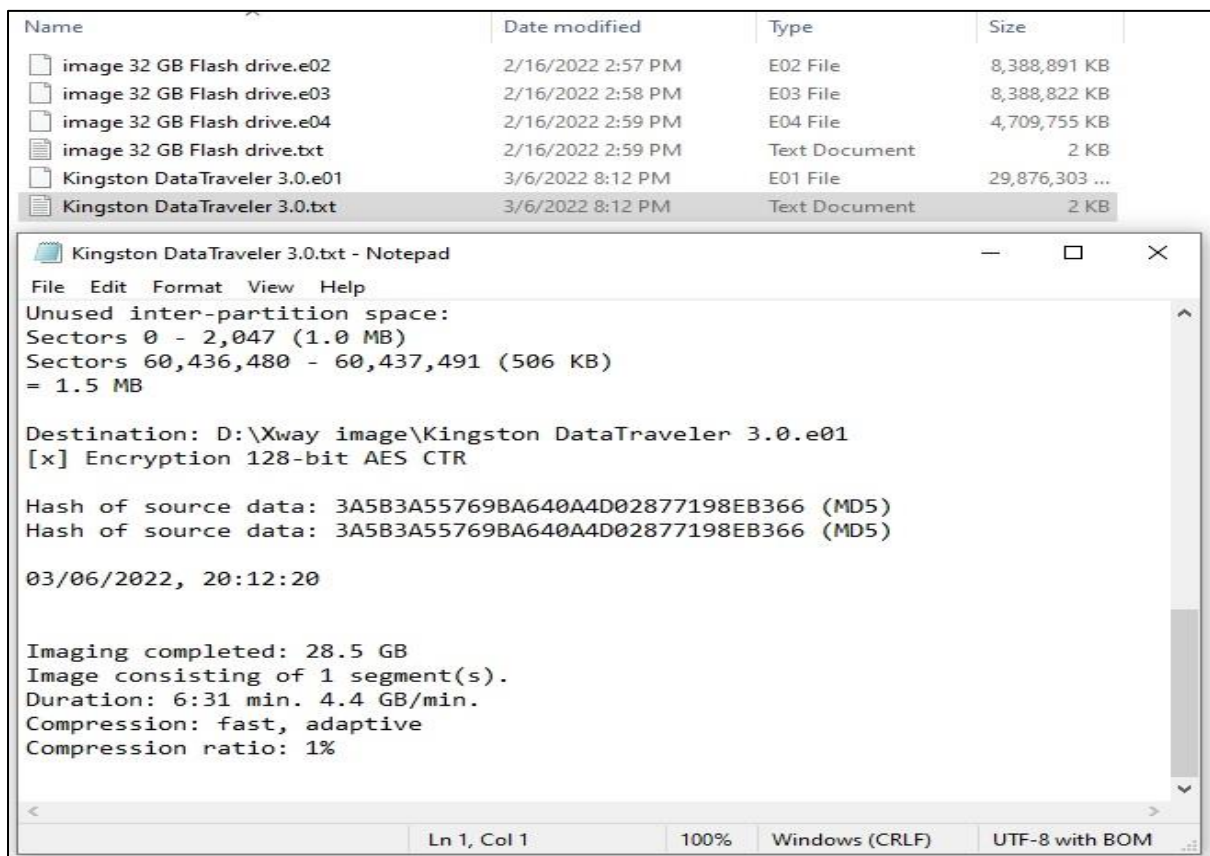


Image ရယူပြီးတဲ့အခါမှာ ရရှိလာတဲ့ Output Result ဖြစ်ပါတယ်။ Text File အနေနဲ့တွေ့ရမှာဖြစ်ပြီး FTK မှာပါတဲ့ အချက်အလက်တွေအတိုင်း ပုံစံအတိုင်းပဲဖြစ်ပါတယ်။

```
image 32 GB Flash drive.txt - Notepad
File Edit Format View Help
02/16/2022, 14:53:40
X-Ways Forensics 20.3 SR-4 x86
Create Disk Image

Computer: PC-2
16 processor cores
Windows 10, Version 20H2
Time zone: +06:30 Myanmar Standard Time
User: acer
Examiner(s): AZM
Internal description: TESTING SPEED AND FILE SYSTEM

Source: Removable medium 1, Partition 1
Sectors 0-60434431

File system: FAT32
Total capacity: 30,942,429,184 bytes = 28.8 GB
Sector count: 60,434,432
Usable sectors: 60,401,664
First data sector: 32,768
Bytes per sector: 512
Bytes per cluster: 16,384
Free clusters: 766,776 = 41% free
Total clusters: 1,887,552
FAT1 = FAT2!
Active FAT(s): All 2
Clean shut down: Yes
I/O error-free: Yes
Serial No.: F48EB5FE (hex)
Serial No.: FEB58EF4 (hex, rev)
Serial No.: 4273311476 (dec, rev)

Destination: D:\Xway image\image 32 GB Flash drive.e01
[x] Split image into segments of 8.0 GB

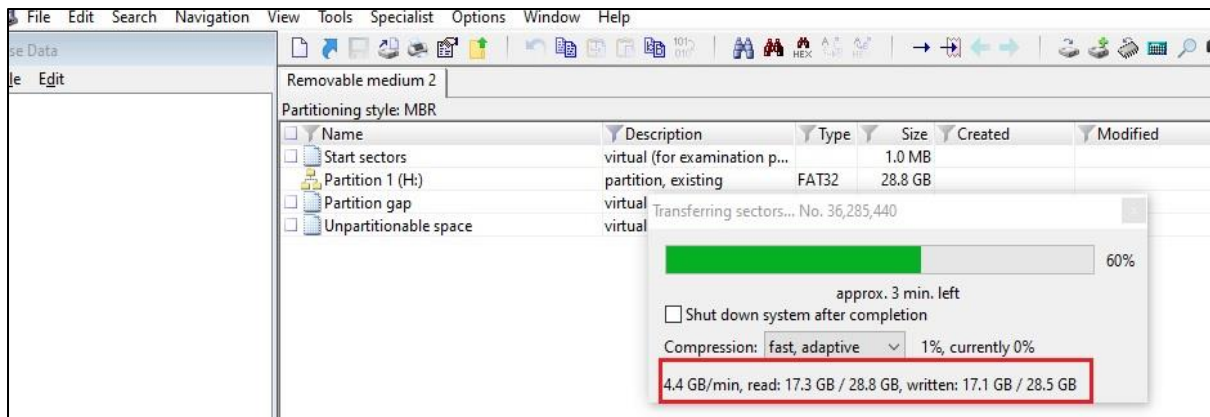
Hash of source data: 02B80A583C6697C1D3E3DD346303F89F (MD5)

02/16/2022, 14:59:55

944,288 chunks
Chunk size: 64 x 512 bytes = 32.0 KB

Segment .e01: 267,760 chunks
Segment .e02: 263,456 chunks
Segment .e03: 262,480 chunks
```

Image Detail Text File



Xway Imager Commercaill Version ဖြစ်တဲ့အတွက် FTK Imager ထက်ပိုပြီး Image လုပ်တဲ့ အချိန်မှာ Speed ပိုမြန်ပါတယ်။

ဒီလောက်ဆိုရင် Digital Forensics Acquisition Process With FTK Imager မှာ FTK Imager ကိုနမူနာထားပြီး ရေးသားတယ်ဆိုတာကို မြင်သာပြီဖြစ်ပါတယ်။ ပိုက်ဆံပေးရတဲ့ Commercial Version တွေကဲ့ကွာခြားမှုအနည်းနည်းသာရှိပြီး တော်တော်များများ ပုံစံတူတာကိုတွေ့ရမှာဖြစ်ပါတယ်။ အသေးစိတ် ကိုတော့ အရင် PDF မှာဖော်ပြထားပြီးသာဖြစ်တဲ့အတွက် မဖော်ပြတော့ပါဘူး။